

University of Groningen

Informatierecht en informatietechnologie

Enneking, P. P. J. L.; Neisingh, A. W.

Published in:
Maandblad voor Accountancy en Bedrijfseconomie

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
1996

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):

Enneking, P. P. J. L., & Neisingh, A. W. (1996). Informatierecht en informatietechnologie: een noodzakelijke combinatie . *Maandblad voor Accountancy en Bedrijfseconomie*, 70(11), 585-589. [2264].

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

Informaticarecht en informatietechnologie: een noodzakelijke combinatie

Mr. P.P.J.L. Enneking en Prof. A.W. Neisingh

THEMA

Inleiding

Ontwikkelingen in gebruik en toepassing van informatietechnologie in organisaties is nog lang niet ten einde. Of ontwikkelingen een modetrend, dan wel een modewoord lijken te zijn zal de geschiedenis moeten uitwijzen. Eén ding is echter in ieder geval zeker. Een juridisch vangnet dient altijd aanwezig te zijn. Niet slechts bedoeld om in geschilsituaties ieders aansprakelijkheid en verantwoordelijkheid met betrekking tot bijvoorbeeld ontwikkeling, onderhoud en/of verwerking van geautomatiseerde toepassingen duidelijk te maken, doch evenzeer om afspraken te maken die duidelijkheid voor alle partijen opleveren zodat daarmee juist geschillen kunnen worden voorkomen.

In de EDP-auditing-praktijk, waarin beide auteurs werkzaam zijn, blijkt bij voortduring dat door het ontbreken van heldere en evenwichtige contracten, zoals licentievoorwaarden, service level agreements, turn-key contracten en dergelijke, partijen vaak in een zeer vervelende positie komen te verkeren. Tijdig voldoende aandacht voor de juridische onderbouwing en evenwichtige vastlegging van de afspraken is derhalve een must.

In dit artikel zal worden getracht aan te geven dat bij de automatisering van organisaties en de uitbesteding van hun geautomatiseerde gegevensverwerking het noodzakelijk is aspecten vanuit de informatietechnologie en vanuit het informaticarecht te combineren teneinde de risico's voor de organisatie in voldoende mate te beheersen. Hierbij worden vooral aspecten geschetst die de auteurs in hun dagelijkse praktijk tegenkomen. Kort worden hierbij behandeld de juridische

aspecten van de selectie en aanschaf van standaardpakketten, het realiseren van maatwerksoftware alsmede de uitbesteding van gegevensverwerking.

Gebruik standaardpakketten

Steeds meer organisaties hebben behoefte aan standaardpakketten, zo nodig aangevuld met enige maatwerkaanpassingen. Aanschaf van standaardpakketten 'off the shelf' zonder een voorafgaande studie en voorbereiding moet in de meeste gevallen echter worden afgeraden, zeker in de gevallen waarbij de automatisering de primaire bedrijfsprocessen ondersteunen. Een gedegen proces van informatie-analyse, globaal ontwerp en functioneel ontwerp dient te worden uitgevoerd om te kunnen vaststellen of de functionaliteit in het standaardpakket geheel, dan wel in belangrijke mate overeenkomt met de specifieke eisen en wensen van de eindgebruiker. Als in de fase van informatie-analyse en inventarisatie van de behoeften, de organisatie om welke reden dan ook hiervoor onvoldoende kwaliteit en kwantiteit kan vrijmaken, zijn organisatie-adviesbureaus en softwarehouses bij uitstek de organisaties die op dit vlak ondersteuning kunnen bieden. Uit deze fase zullen de eisen en wensen van de organisatie en de (eind)gebruikers moeten worden gededistilleerd, zodat een betere en meer verantwoorde keuze van het pakket kan worden gemaakt. De door de organisatie gewenste functionaliteiten en

Mr. P.P.J.L. Enneking en Prof. A.W. Neisingh zijn werkzaam bij KPMG EDP Auditors en adviseren organisaties over aspecten van informatietechnologie en informatiebeveiliging, in combinatie met aspecten van informaticarecht.

specificaties moeten immers 'matchen' met hetgeen het uiteindelijk te kiezen pakket biedt. Voorts zal de omschrijving van de aan het pakket te stellen functionaliteiten, specificaties en andere eisen, een belangrijk onderdeel worden van het te sluiten contract met de softwareleverancier.

Tijdens de volgende stappen heeft de organisatie veelal behoefte aan een fulltime projectleider, zo leert de praktijk. Immers, de informatie-analyse dient nader te worden geconcretiseerd en gedocumenteerd, waarbij opnieuw behoefte kan bestaan bij de organisatie om derden in te schakelen bij de uitwerking en haar te begeleiden bij de definitieve pakketkeuze. Wanneer een project een redelijke omvang dreigt te krijgen, kan het verstandig zijn reeds in een vroegtijdig stadium bijvoorbeeld extern een projectleider aan te trekken.

In het proces van opleveren van functionele specificaties en het ondersteunen van de organisatie om te komen tot een selectie van pakketleveranciers treffen wij naast organisatie-adviseurs en softwarehouses uiteraard ook EDP-auditors aan.

De laatsten hebben hun kennis met betrekking tot het onderhavige gebied nogal eens verkregen uit het feit dat pakketten door EDP-auditors worden beoordeeld en hebben gerapporteerd ter zake van de kwaliteit (betrouwbaarheid en continuïteit). Beoordeling en rapportering geldt niet slechts voor financiële administratieve systemen, doch evenzeer voor betrouwbaarheidsaspecten en beveiligingsaspecten, opgenomen in logistieke programmatuur. Bij EDP-auditors aanwezige kennis op dit terrein blijkt vaak, misschien wel te vaak, te worden onderschat.

Als beoordelingscriterium bij de selectie van standaardpakketten dient in ieder geval in een vroegtijdig stadium 'het contract' te worden betrokken. Maar al te vaak blijkt namelijk dat de heldere en evenwichtige vastlegging van de door de softwareleverancier voorgespiegelde toezeggingen en beloften over bijvoorbeeld performance en specifieke kwaliteiten van het pakket in het geheel niet of veel te laat plaatsvindt. Veelal wordt volstaan met een beknopte vastlegging van prijs en betalingscondities onder verwijzing naar de algemene (licentie)voorwaarden en andere kleine lettertjes. Wanneer dan na ingebruikname van het pakket blijkt dat dit op een of meer punten toch niet helemaal voldoet aan de in het voortraject gedefinieerde behoeften en eisen, zal in negen van de tien gevallen blijken dat de afnemer in juridisch

opzicht geen poot heeft om op te staan. Hetzelfde probleem speelt zodra blijkt dat implementatie toch iets ingewikkelder is dan aanvankelijk was gedacht en een forse uitloop in tijd en kosten ontstaat.

Overigens is het vanuit de zijde van de leverancier gezien vaak ook verstandig tijdig 'het contract' ter sprake te brengen, met name ten aanzien van de punten performance en specifieke kwaliteiten en functionaliteiten. Door vroegtijdig duidelijkheid te verkrijgen over de wijze waarop het te leveren product past bij de wensen en verwachtingen van de afnemer kunnen veel problemen immers worden voorkomen. De ervaring leert echter dat het juist bij standaardpakketten nog al eens voorkomt dat vanuit de leverancier meer wordt gelet op de omzetscore dan op de uiteindelijke klanttevredenheid.

De vast te leggen afspraken en spelregels zijn in feite allemaal gericht op het conform de planning door de leverancier opleveren van een systeem of pakket dat voldoet aan de overeengekomen functionaliteiten en specificaties. In dit verband zou dus gesproken moeten worden van een resultaatsverbintenis van de leverancier en niet van een inspanningsverplichting zoals veelal in de algemene voorwaarden van de softwareleveranciers tot uitdrukking wordt gebracht. In de contractuele afspraken zullen derhalve - naast de nodige 'algemene juridische' spelregels - duidelijke garanties moeten worden opgenomen ten aanzien van planning, te realiseren functionaliteiten en specifieke voor de organisatie van belang zijnde eisen en wensen zoals deze in het voortraject zijn vastgesteld. Voorts zal een sluitende regeling moeten worden getroffen met betrekking tot een acceptatieprocedure, aan de hand waarvan de door de leverancier te leveren prestaties zullen worden getoetst.

De beschrijvingen van de functionaliteiten, performance- en kwaliteitseisen en andere specificaties zullen veelal in een bijlage bij de overeenkomst worden opgenomen. Dat is ook wel logisch, doch onze ervaring is dan dat het belang van deze bijlagen te zeer wordt onderschat. In de overeenkomst kunnen dan wellicht spijkerharde resultaatsverplichtingen zijn opgenomen; als dan vervolgens de uitwerking daarvan (in de bijlage) in ogenschouw wordt genomen, blijkt dat vaak is volstaan met een algemene en dus niet op de specifieke situatie toegesneden formulering zoals bijvoor-

beeld 'normaal gebruikelijke performance-eisen'. In het ergste geval blijkt soms over de gewenste kwaliteit of specificatie in het geheel niets te zijn vastgelegd. Overigens moet men zich realiseren dat het andere uiterste, dat wil zeggen letterlijk alles willen vastleggen, veelal niet verstandig is en ook niet mogelijk is.

De in het voortraject getroffen voorbereidingen, de inventarisatie van eisen en wensen, de definiëring van functionaliteiten en performance-eisen zullen als basis moeten dienen voor de vastlegging van de afspraken en daarmee het formuleren van de uiteindelijke bijlagen bij het contract zeer vergemakkelijken.

Wordt uiteindelijk overgegaan tot aanschaf van een standaardpakket, dan zou de organisatie toch tenminste wensen dat er ook een zekerheid met betrekking tot de continuïteit van de organisatie van het software house en van het onderhoud van het pakket zal bestaan. Software wordt in de meeste gevallen namelijk in zogeheten 'object-vorm' geleverd, waardoor het voor de afnemer onmogelijk is in geval van calamiteiten zoals faillissement of wanprestatie van de leverancier, zelfstandig het onderhoud uit te voeren. Een forse afhankelijkheid van de vakkundigheid en de continuïteit van leverancier is derhalve het gevolg. Een escrow-procedure¹ zal dan ook deel moeten uitmaken van het contract. EDP-auditors zijn nogal eens betrokken bij de uitvoering van escrow-procedures, met name daar waar het gaat om de vaststelling dat door de pakketleverancier daadwerkelijk de broncode en alle verdere relevante informatie is gedeponneerd zodat de afnemer in staat is wel zelfstandig (of met inschakeling van een ter zake deskundige) het onderhoud uit te voeren. Er is hier sprake van zogeheten actieve escrow.

Een escrow-overeenkomst dient juridisch voldoende sluitend te zijn om te waarborgen dat in geval van conflict of faillissement ook daadwerkelijk de broncode en relevante informatie beschikbaar komt. Voorts zal moeten worden vastgelegd dat de organisatie ook gerechtigd is de broncode te gebruiken en gerechtigd is voor verder onderhoud derden in te schakelen.

Reeds in het begin van dit onderdeel werd gesproken over maatwerkaanpassingen. Het komt nog weleens voor dat de gewenste functionaliteit niet geheel overeenkomt met hetgeen door het standaardpakket wordt geboden. Aan het realise-

ren van maatwerkaanpassingen dient in de overeenkomst zonder meer de benodigde aandacht te worden besteed. Het spreekt voor zich dat een volledige beschrijving van de te realiseren functionaliteiten en de aan de programmatuur te stellen eisen een wezenlijk onderdeel van het contract zal uitmaken. Wanneer anderen dan de leverancier van het standaardpakket de additionele functionaliteit ontwikkelen, zal aan de orde moeten komen wie verantwoordelijk is wanneer het totaal op enig moment niet blijkt te voldoen aan de overeengekomen specificaties en eisen. Voorkomen dient te worden dat de leverancier van het standaardpakket en de bouwer van het maatwerk elkaar de zwarte piet toeschuiven en uiteindelijk de afnemer op geen enkele wijze verhaal heeft.

Voorts dienen met de maker van de programma's afspraken over intellectueel eigendom te worden gemaakt. Doet men dit niet dan komt krachtens de Nederlandse Auteurswet de intellectuele eigendom van de programma's toe aan de maker², ondanks dat de afnemer de programma's volledig financiert!

Maatwerk

Het komt nogal eens voor dat een organisatie niet uit de voeten kan met de in de markt aangeboden standaardoplossingen, ook niet indien enkele maatwerkaanpassingen worden doorgevoerd. Voor de specifieke bedrijfsprocessen zijn deze organisaties dan genoodzaakt de geautomatiseerde informatieverzorging zelf te ontwikkelen. Dit gebeurt met name in organisaties die als enige bepaalde activiteiten ontplooiën of in die organisaties die zich in een markt bewegen waarin iedere concurrentievoorsprong van wezenlijk belang is, en waarin automatisering derhalve van strategische betekenis is.

Externe adviseurs, software houses, EDP-auditors en anderen kunnen dan in de verschillende fasen van ontwikkeling worden ingeschakeld. Een situatie die zich hier nogal eens voordoet is dat software houses onderaannemers gebruiken voor bijvoorbeeld programmatuurontwikkeling. In dat geval is het van wezenlijk belang dat de hoofdaannemer de eindverantwoordelijke blijft voor de realisering van het overeengekomen resultaat. Voorkomen dient te worden dat de organisatie de dupe wordt van verschillende partijen die elkaar verantwoordelijk houden voor

onverhoopte fouten in de software of uitloop in de planning.

Duidelijke afspraken dienen met software-ontwikkelaars te worden gemaakt met betrekking tot het gebruik van software-ontwikkel-tools, ontwikkelplatforms en dergelijke. De opdrachtgever loopt grote risico's wanneer zijn project als een soort proeftuin wordt gebruikt voor het opdoen van kennis en ervaring met betrekking tot nieuwe ontwikkelomgevingen.

Bij projecten van dergelijke omvang is het voor organisaties van grote betekenis de kwaliteitsbeheersing door onafhankelijke derden te laten plaatsvinden. Met name EDP-auditororganisaties hebben deskundigheid in huis op het terrein van Quality Assurance, Quality Engineering en Quality Control.³ Ook met dergelijke onafhankelijke deskundigen dienen goede afspraken te worden gemaakt.

Tijdens het proces van het ontwikkelen van maatwerk kan het gewenst zijn invoeringsscans dan wel projectscans te laten uitvoeren door deskundigen om daarmee inzicht te krijgen in de status van het project, de kwaliteit, de voortgang en uiteindelijk of het al dan niet verantwoord zou zijn op een bepaalde datum tot invoering over te gaan.

Voorts zouden deze onafhankelijke deskundigen een rol kunnen spelen in de acceptatieprocedure. Uit de acceptatietest(s) moet immers blijken in hoeverre de overeengekomen functionaliteiten zijn gerealiseerd en is voldaan aan de overeengekomen kwaliteits- en performance-eisen die zijn vastgelegd in de bij het contract behorende bijlagen.

Uitbesteding gegevensverwerking

In de strategiediscussies van organisaties speelt met name in de afgelopen jaren een rol zich te willen beperken tot de kernfunctie van het bedrijf. In een groot aantal gevallen past de geautomatiseerde gegevensverwerking niet in de kernfunctie van zo'n organisatie, waarop vervolgens tot uitbesteding van de geautomatiseerde gegevensverwerking wordt overgegaan. Naast contractuele afspraken die tussen uitbesteder en Rekencentrum dienen te worden vastgelegd geldt in het bijzonder dat allerlei details in service level agreements worden overeengekomen. Met name indien bij de uitbesteding de uiteindelijke controle en de beheersing van de gegevensverwerking aan het Rekencentrum wordt overgedragen wordt de

afhankelijkheid van de deskundigheid en de continuïteit van dat Rekencentrum zeer hoog. Daarom is het van wezenlijk belang dat voldoende aandacht wordt besteed aan de contractuele aspecten en aan de nauwkeurige vastlegging van de gewenste kwaliteiten en prestaties. De uitgangspunten hierbij zijn feitelijk identiek aan hetgeen hierboven bij de aanschaf van pakketten werd gememoreerd: de afspraken zijn in feite allemaal gericht op het conform de planning door de leverancier opleveren van zekere prestaties of producten die voldoen aan de overeengekomen functionaliteiten en specificaties en andere specifieke eisen.

Juist op deze vlakken blijken in de praktijk nog al eens vragen aan EDP-auditors te worden voorgelegd teneinde meer zekerheid te verkrijgen over de wijze waarop de administratieve organisatie na de uitbesteding moet worden ingericht en daarmee de risico's die met uitbesteding samenhangen beter te beheersen. Bij het onderzoek worden dan vaak ook aspecten meegenomen inzake de correctheid van de in rekening gebrachte bedragen en ten aanzien van de naleving van wettelijke voorschriften zoals bijvoorbeeld verplichtingen uit hoofde van de privacyregeling, administratieve- en bewaarverplichtingen en de Wet computercriminaliteit.

Ook in deze gevallen zien we dus een belangrijk raakvlak tussen juridische aspecten van informatietechnologie, de kwaliteit van de IT en de beantwoording van specifieke vragen.

Er is overigens een tendens waarneembaar, waarbij binnen concernverband tot uitbesteding wordt overgegaan en in concernverband service level agreements worden afgesloten met de bedrijfsonderdelen die de dienstverlening bij een gemeenschappelijk Rekencentrum hebben uitbesteed. Het is zaak ook aan deze service level agreements de benodigde aandacht te besteden ondanks dat dit veelal 'interne concernafspraken' betreft. Wanneer immers enig bedrijfsonderdeel wordt vervreemd gebeurt het niet zelden dat het reeds bestaande service level agreement onderdeel zal uitmaken van het koop/verkoopcontract.

Conclusie

De praktijk leert dat bij de automatisering van organisaties, bijvoorbeeld bij de aanschaf van standaardpakketten en de vervaardiging van

maatwerk, maar ook bij de uitbesteding van gegevensverwerking veelal te laat en ook onvoldoende aandacht wordt besteed aan een heldere en evenwichtige vastlegging van hetgeen is overeengekomen. Met het vastleggen van de rechten en verplichtingen van partijen blijkt veel ellende te kunnen worden voorkomen, omdat dan tevoren duidelijk is wat partijen van elkaar kunnen en mogen verlangen, maar ook wat partijen juist niet van elkaar hoeven te verwachten.

Bij het vastleggen van de afspraken blijkt een nauwkeurige formulering van de overeengekomen functionaliteiten, performance-eisen en andere specificaties nogal eens over het hoofd te worden gezien dan wel onvoldoende gewicht te krijgen omdat deze zaken veelal in bijlagen zijn verscholen. Door een gecombineerde aandacht aan aspecten van informatietechnologie en informatie-recht bij de selectie van een pakket- of diensten-leverancier en bij de invoering hiervan in de organisatie van de afnemer, zouden deze proble-

men kunnen worden voorkomen en kunnen automatiseringsrisico's beter worden beheerst.

NOTEN

1 In het kader van een escrow-procedure worden de source-codes, ontwikkeldocumentatie en andere relevante informatie ten aanzien van de software gedeponeerd bij een onafhankelijke derde (escrow-agent). Met behulp van het gedeponeerde materiaal (dat voor de leverancier wezenlijke bedrijfsgeheimen bevat) kan de afnemer zelfstandig het onderhoud uitvoeren. Zodra zich een in de escrow-overeenkomst omschreven afgiftegrond voordoet (bijvoorbeeld faillissement of wanprestatie in het onderhoud) is de escrow-agent verplicht het gedeponeerde materiaal aan de afnemer af te geven.

2 Aldus art. 1 Auteurswet 1912.

3 Zie voor een beschrijving van deze begrippen het artikel in Compact 1990 nr 2 pp. 3 t/m 13 van Laurent Gielen en Frits Swinkels.